IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	:	Case No. 1:18-cr-00043
	:	
Plaintiff,	:	Judge Timothy S. Black
	:	
vs.	:	
	:	**DEFENDANT'S MOTION FOR**
YANJUN XU,	:	**JUDGMENT OF ACQUITTAL**
a/k/a Xu Yanjun,	:	
a/k/a Qu Hui,	:	
a/k/a Zhang Hui,	:	
	:	
Defendant.	:	
	:	

Defendant Yanjun Xu ("Mr. Xu") moves the Court for a judgment of acquittal, pursuant to Federal Rule of Criminal Procedure 29(a). The government's evidence closed with the government failing to present sufficient evidence that Mr. Xu committed the crimes charged in the indictment.

"[T]he court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction." Fed. R. Crim. P. 29(a). The Court must consider whether—at the time of the motion, and viewing the evidence in the light most favorable to the government—there is sufficient, relevant evidence from which a reasonable jury could find the defendant guilty beyond a reasonable doubt. *United States v. Adan*, 913 F. Supp. 2d 555, 563 (M.D. Tenn. 2012), *aff'd sub nom. United States v. Fahra*, 643 F. App'x 480 (6th Cir. 2016). The government failed that test here.

ARGUMENT

The government charged Mr. Xu in a four-count indictment, alleging that he attempted and conspired to violate the Economic Espionage Act ("EEA"), 18 U.S.C. § 1831 et seq. (the "Indictment"). Counts I and II alleged conspiracies to commit economic espionage and to steal

trade secrets, beginning in 2013, continuing to April 1, 2018. Counts III and IV allege attempts to commit economic espionage against and to steal trade secrets from General Electric Aviation ("GE Aviation") between March 2017 and April 2018.

I. The Government has not proven that Mr. Xu joined a conspiracy with the criminal objective of stealing trade secrets.

Counts I and II of the Indictment require the government to prove, *inter alia*, that Mr. Xu and at least one other person formed an agreement to "knowingly" steal a trade secret. 18 U.S.C. §§1831(a)(5) and 1832(a)(5). The EEA defines "trade secret" as information that (a) the owner has taken reasonable measures to keep secret, *and* (b) derives independent economic value from not being generally known to or readily ascertainable by "another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3).

The essence of a conspiracy is an agreement, but not just any agreement will do. It must be an agreement to accomplish some definite, illegal *object*. *See United States v. Lopez-Medina*, 461 F.3d 724, 747 (6th Cir. 2006) (holding that to prove the existence of a conspiracy, the prosecution must establish, *inter alia*, that there was "an object to be accomplished.") (quotations omitted); *United States v. Rosenblatt*, 554 F.2d 36, 39 (2d Cir. 1977) ("Thus, it is clear that a general agreement to engage in unspecified criminal conduct is insufficient to identify the essential nature of the conspiratorial plan.")

So in order to convict Mr. Xu of counts I and II of the Indictment, the government must prove beyond a reasonable doubt that Mr. Xu and at least one other person formed an agreement to "knowingly" steal what they believed to be trade secrets—information that the owner tried to keep secret, and that derived its value from being secret. *United States v. Liew*, 856 F.3d 585, 597 (9th Cir. 2017). Additionally, to convict Mr. Xu on Count II (theft of trade secrets), the

government must also prove beyond a reasonable doubt that the alleged conspirators knew or intended to injure the owner of the trade secret. 18 U.S.C. § 1832(a).

This means that the government must do more than prove that the alleged conspirators sought out "information"—or even non-public, non-trade secret information. Rather, the government must show a specific intent to unlawfully obtain trade secrets.

The government's theory of the case on the conspiracy counts has shifted over time. Initially, the government focused on what it alleged to be efforts to steal trade secret information from GE Aviation in 2017-2018. The government alleged that this conspiracy operated by inviting foreign experts to China to give presentations (termed "exchanges") on aviation technology. (Indictment, Doc. 1, ¶ 13(h), at PageID #7.) The government later announced a shift: it proposed that part of the conspiracy involved "hacking" a computer belonging to an employee of French aerospace company Safran S.A. (Notice of 404(b) Material, Doc. 88, at PageID #908.) But one thing is consistent: There's no evidence that the conspiracy—however defined—had the specific criminal objective of unlawfully obtained trade secrets.

A. The Safran intrusion does not reflect an intent to steal trade secrets.

The government offers two bits of evidence to show the criminal objective of the alleged conspiracy, but neither does the job. The first is the Safran hacking incident, which the government suggests both is a part of the alleged conspiracy and demonstrates an intent to steal trade secrets. (Response to Defendant's Motion in Limine, Doc. 128, at PageID #1562-1565.) According to the government's theory, Chinese agents planted malware on the computer of a Safran employee who was working *in China* at the time, between January and April 2014. (*Id.*) But the government's own witness, Agent Adam James, testified that he could not determine if any documents were targeted or accessed during the hack, that no files were exported from the Safran system, and that he had no evidence that anyone tried to download or export a trade

secret. In fact the government did not introduce evidence that the laptop had any trade secrets on the hard drive. So despite having access to the Safran computer for three months, and—in the government's telling—the *motive* to steal trade secret information, none of the alleged conspirators stole any trade secrets.[1]

Agent James also testified that MSS is responsible for domestic security, particularly rooting out internal spies in China, and monitoring companies and foreigners in China. He further testified that to achieve those ends, China uses several techniques, including bugging or intruding into a computer so that China could conduct surveillance. The Safran intrusion is far more consistent with surveilling the foreign employee working in China than with any effort to steal trade secrets. So if anything, the Safran intrusion shows that the alleged conspiracy did *not* form the specific criminal intent to steal trade secrets (nor the intent to steal trade secrets *so that* or *knowing that* the theft would injure the owner of the secrets).

B. James Olson's testimony does not establish a criminal intent to steal trade secrets.

The only government witness who testified to any specific intent was James Olson. Olson opined that MSS seeks information, including trade secret information. But there are three independently fatal flaws in his testimony. The first is that, by his own admission, he does not know anything about how MSS operates. He has been out of intelligence for 22 years—and even when he was an active agent, he focused on Cold War Russia (which he admitted was culturally closer to the US than either is to China). He does not know how anything about the MSS organization including its size, how MSS trains its agents, who trains its agents, what it trains its

[1] Agent James also read communications from Tian, Gu, and between MSS colleagues—none of the communications referenced an effort to obtain documents or steal trade secrets, nor did they mention composite materials, fan blades, or aviation technology.

agents to do, or what kind of alleged "spycraft" it employs. So it is hard to imagine that he could competently testify about the organization's intentions—much less that it has the specific criminal intent to steal aviation trade secrets.

Second, Olson testified that virtually all of Mr. Xu's alleged conduct is perfectly legal and consistent with an organizational mission to gather information that is not specifically trade secrets. In particular, academic exchanges like the one with Zheng at the center of this case are both common and lawful. According to Olson, there is nothing untoward about using multiple email addresses or multiple names. There was nothing untoward about Mr. Xu's proposed meeting with Zheng in Belgium: The government hangs much on the fact that Mr. Xu had photos of Zheng and brought $7000 with him to Belgium. But Mr. Xu and Zheng were friends on social media; the fact that Mr. Xu had photos would not be indicative of spycraft (nor, contrary to the government's suggestion, would it be a wise or useful tool for intimidating someone into giving up trade secrets—not that Mr. Xu attempted to do so). And, according to Olson, $7000 is not enough to buy your way into a trade secret worth untold millions (that amount is, however, perfectly consistent with reimbursing someone for a transcontinental flight or shopping in Europe).

Third, Olson himself testified that China is behind the US in science and technology, and seeks out information of all kinds wherever they can find it. But a broad organizational mission to find "information"—much of which, Olson agreed, is open source intelligence—is hardly indicative of a specific criminal objective to steal trade secrets. Further, if Olson is right and China is simply seeking to catch up to American technology, then the alleged conspiracy could not have acted with the specific knowledge and intent to injure the corporate owners of trade secrets, as required for a conviction on Count IV.

By his own admission, Olson's testimony is largely based on the limited selection of communications that the government fed him. He admitted that Mr. Xu's conduct is not by itself indicative of spycraft;[2] he only believed it was spycraft because the government told him that Mr. Xu was a spy. But if one removes the government's shading of the witness, Mr. Olson simply could not and did not describe anything criminal about Mr. Xu's conduct.

II. The Government has not proven that Mr. Xu formed the criminal intent to steal a trade secret.

Counts III and IV, the attempt counts, are even more specific. They are tied to interactions with a GE Aviation engineer between 2017 and 2018. The government must show that Mr. Xu specifically intended to unlawfully obtain trade secrets, and that he took a "substantial step" towards carrying out the offense. That step must be beyond mere preparation, and must demonstrate Mr. Xu actually intended to complete the substantive crime. *United States v. Yang*, 281 F.3d 534, 543 (6th Cir. 2002). And Count IV, like Count II, requires the additional showing that Mr. Xu knew or intended for his conduct to injure GE Aviation. 18 U.S.C. § 1832(a).

The attempt counts are specific to GE Aviation and the "exchange" in which Zheng (a GE Aviation engineer) was invited to give a presentation in China. The question is straightforward: Where does the evidence show that Mr. Xu formed the specific criminal intent to steal trade secret information from GE Aviation, and when did he take a "substantial step" towards that goal?

[2] Even if it were, "spycraft" is not the same thing as a specific criminal objective to steal trade secrets.

A. The 2017 Exchange does not involve any request or attempt to obtain trade secrets from GE Aviation.

Zheng testified extensively about his interactions with Mr. Xu and Chen Feng, and nowhere does he describe an attempt to obtain trade secrets. Chen connected to Zheng via LinkedIn—a perfectly ordinary use of the platform. The two started communicating via email in March of 2017; the government read many of those emails into evidence as exhibit 60b. Zheng was planning to visit family in China in May of 2017, and said he could stop by the National University of Aeronautics and Aerospace – a prestigious university which Zheng considered an honor to be invited. (Ex. 60b, at 3.) Chen suggested that he give a presentation on composite materials in aircraft engines. Zheng said that he had to sign a technical agreement with GE, and that technical or proprietary information could not be shared. (Id. at 12.) Chen said that he respected the policy and said he would be happy to have Zheng only discuss general topics that would not violate GE's policies. (Id. at 18.) That is, Chen affirmatively disclaimed any interest in any information that GE took steps to keep secret, and thus disclaimed any interest in trade secret information.

Zheng prepared a presentation based on public information he pulled from professional and academic journal articles. He also zipped five files (training documents) that were GE proprietary information. Chen had never asked for that information, and Zheng testified that he took measures to protect against disclosure and did not share them or present on them. Zheng met with Chen, Qu Hui (whom the government believes is Mr. Xu), and others for both morning tea and lunch—no one asked Zheng about his work or any proprietary information.[3] He delivered a one and one-half hour presentation to 25 students and professors in the afternoon—Zheng

[3] Zheng testified that no one accessed his laptop while he was in China, and that the 5 proprietary training documents he took with him (of his own accord) were not released.

again did not disclose any proprietary information. After the presentation, he was given $3500 for his plane ticket and for the presentation—an amount Zheng thought was perfectly reasonable for the trip and presentation.

Nowhere in Zheng's testimony about the 2017 exchange does he describe any effort by Mr. Xu (or anyone else) to get him to disclose trade secret information.

B. None of the post-exchange communications involve a request or attempt to obtain trade secret information.

On November 1, 2017, Zheng started cooperating with the FBI. From that point on, Zheng was merely a conduit for the government's communication with Chen and Mr. Xu. At the government's behest, Zheng reached out to reestablish contact with Chen in late 2017. They discussed a second exchange; Chen said they were not in a rush because NUAA was on break, and suggested that he talk to Mr. Xu about finances. (Ex. 67c). During that conversation, Zheng (on behalf of the government) repeatedly asked what information NUAA wanted for the exchange; Mr. Xu told him multiple times that he did not have to prepare or do *anything*. *(Id.*)

Apparently dissatisfied with Mr. Xu's failure to climb into the trap and ask for trade secrets, the government decided to offer them of its own accord. For example, after Mr. Xu told Zheng he did not need to bring or prepare any materials, Zheng sent a message (on behalf of the FBI) showing that he could get information right away. FBI Agent Bradley Hull testified that the message was an offer to Mr. Xu to try to bait him into asking for specific information. But the ask never came. Indeed, the only time proprietary information came up was when Zheng (on behalf of the FBI) offered a document that the FBI doctored with "GE Designation: Confidential" in order to entice Mr. Xu to ask for it. (Ex. 68.) Agent Hull testified that he sent the document in order to keep Mr. Xu's interest. In his response, Mr. Xu clearly did not

understand what Zheng (or the FBI) had sent him. (Ex. 69.) So he offered to connect him with experts in China.

The closest the government comes to even suggest a request for a trade secret is in Exhibit 70, where Mr. Xu asks Zheng to sort out a directory of his computer. But a computer directory is not "trade secret information" as defined in the EEA—nor would anyone reasonably believe that the directory of a laptop "derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[4] Mr. Xu later asked for "more data," but never asked for trade secret information (or for anything that could have been construed as trade secret information). (Ex. 67c.) The government (through Zheng, and with GE's consent) sent a purported "design" document to Mr. Xu with a designation "GE Proprietary Information." But Mr. Xu had not asked for it, or for any proprietary or trade secret information from GE.

The government will no doubt try to make much of Mr. Xu's trip to Belgium to meet with Zheng and receive the directory of his computer. But it must be stressed again that Mr. Xu did not ask for trade secret information—nor would he have any reason to believe that the directory itself was a trade secret. And so the mere fact that he met Zheng in Europe to receive that non-trade secret information does not convert the information into a trade secret.

CONCLUSION

The jury could convict Mr. Xu only if the government proves beyond a reasonable doubt that Mr. Xu formed the specific criminal intent to steal what he believed to be a trade secret. The government's theory seems to be that Mr. Xu is a spy and spies steal things, so he must be guilty.

[4] That request came only after the government's efforts to bait Mr. Xu.

But that is not what the EEA requires. The government has not established any agreement or the specific criminal objective of the charged conspiracy, nor has it proven the specific criminal intent required for the attempt charges. As a result, the Court should enter a judgment of acquittal on all charges.

Respectfully submitted,

/s/ Ralph W. Kohnen
Ralph W. Kohnen (0034418)
Jeanne M. Cors (0070660)
Robert K. McBride *(pro hac vice)*
Sanna-Rae Taylor (0091302)
Taft Stettinius & Hollister LLP
425 Walnut Street, Suite 1800
Cincinnati, Ohio 45202-3957
Telephone: (513) 381-2838
Fax: (513) 381-0205
kohnen@taftlaw.com
cors@taftlaw.com
rmcbride@taftlaw.com
srtaylor@taftlaw.com

Florian Miedel *(pro hac vice)*
Miedel & Mysliwiec LLP
80 Broad Street, Suite 1900
New York, NY 10004
Telephone: (212) 616-3042
Fax: (800) 507-8507
fm@fmamlaw.com

COUNSEL FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that on November 1, 2021 a copy of the foregoing was filed electronically. Notice of this filing will be sent to all parties in this case by operation of the Court's CM/ECF system. Parties may access this filing through the Court's system.

/s/ Ralph W. Kohnen